=====================================================
===============

HIPAALERT -- Volume 3, Number 7 -- July 22, 2002

>>From Phoenix Health Systems--HIPAA Knowledge--HIPAA Solutions<<
=> Healthcare IT Consulting & Outsourcing <=

=====================================================
===============

HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total over 18,000.

=====================================================
===============

=====================================================
===============

## THIS ISSUE

=====================================================
===============

## 1 >> FROM THE EDITORS:

Historically, the healthcare industry tends to experience a slowdown in new initiatives during July and August -- serious vacation months for many. However, and though the official results of our Summer Quarterly HIPAA Survey are not yet in, early indicators are that most industry sectors are more "fired up" than ever when it comes to HIPAA remediation planning and project start-ups. And many that have not yet begun impact assessments are anxiously seeking the simplest and fastest approaches to this preliminary compliance step.

What's generating the unusual hot summertime momentum? One reason may be

HHS'comments that we can expect to see a final Security Rule and updated Privacy Rule as early as August. But an even stronger factor is DEADLINES. They are, essentially, upon us. The original Transactions deadline (also, now, the deadline for filing an extension request and compliance plan) is less than three months from now. The Privacy compliance deadline and Transactions testing deadline are little more than half a year away. Hot weather or cold, vacation season or not, most of us are acknowledging there's no time left to waste!

D'Arcy Guerin Gue, Publisher
dgue@phoenixhealth.com

Bruce Hall, Director of Internet Services
bhall@phoenixhealth.com

==================================================================

2 >> HIPAAnews

** Arguments Expected on HIPAA Privacy Lawsuit **

Oral arguments are expected early next month in a suit filed last year challenging the medical privacy rule, reports Health Data Management. Court arguments in the case filed by two state medical societies in U.S. District Court in Columbia, S.C. come as HHS prepares in August to publish a final rule modifying the privacy rule.

Read more: http://www.hipaadvisory.com/news/index.cfm#0719hdm

** House Leadership Bows to President on Security Dept.,
But Opposes Possible National ID Card **

The New York Times reports Republican leaders of the House said last week that they planned to give the Bush administration almost all it wanted in a new Department of Homeland Security. A draft of the agreed-to bill closely hews to the changes the White House had said it would accept. The White House, however, did not get everything it hoped for. House leaders do not agree with an administration proposal for a nationalized driver's license, which could become a national identification card. Conservative and liberal privacy advocates alike opposed this idea.

The bill would also block the proposed transfer of the computer security division of the National Institute of Standards and Technology (NIST) to the Homeland Security Department. The draft generated by the House Select Homeland Security Committee instead establishes a new cybersecurity program.

Read more: http://www.hipaadvisory.com/news/index.cfm#0719nyt

** Eckerd Must Endow Ethics Chair to Settle Ethics Complaint**

The Miami Herald reports the Eckerd drug store chain recently agreed to pay $1 million to bankroll an ethics chair at Florida A&M University's (FAMU) school of pharmacy to settle a complaint that it had misled customers about its marketing efforts. An investigation was launched after it was learned that when customers signed a slip acknowledging they were receiving a prescription drug, the fine print included authorization to release information to Eckerd for future marketing purposes. Meanwhile, Bush administration officials are seeking to modify provisions of the healthcare privacy act to make it easier for pharmacies to use customer information for marketing purposes.

Read more: http://www.hipaadvisory.com/news/index.cfm#0718mh

** Kennedy's eHealth Act Would Require CPOE in Hospitals **

The California Healthcare Foundation's iHealthBeat reports that under the proposed federal eHealth Act, hospitals would be required to use computer physician order entry (CPOE) systems in order to receive payments from federal health plans. The requirement would take effect five years after the bill's passage, for hospitals that admit more than 20,000 patients annually, and 10 years after the bill's passage for all hospitals. Sen. Edward Kennedy (D-MA), chair of the Senate Health, Education, Labor and Pensions (HELP) Committee, introduced the Efficiency in Health Care -- or eHealth Care -- Act on June 18, but details of the bill S. 2638 only recently became available.

Read more: http://www.hipaadvisory.com/news/index.cfm#0717ken

=========================================================================

3 >> HIPAAction: Feature Article

** Patient Access: "Getting HIPAA Right" **

by John Thompson, Phoenix Health Systems

In health care organizations (HCOs), almost every department will be affected by HIPAA compliance. However, few departments will be impacted as directly as those that provide patient access services, particularly with regard to Privacy. This is primarily due to patient access areas' front-end role in collecting billing and demographic data, as well as general consents. Fortunately, there are practical, inexpensive solutions that access managers can deploy to achieve HIPAA compliance, some of which have an added benefit of enhancing delivery of customer service.

------------------------
Consent: Keep it Simple

The Privacy Rule requires written consent by a patient before covered entities may use or disclose the patient's protected health information (PHI) to perform treatment, payment or healthcare operations (TPO). Most HCOs currently have language in their general consent forms that authorize release of information to insurance companies and other parties involved in billing and collections activities.

One suggestion for patient access managers: determine how simple modifications may be made to existing general consent forms, for allowing the use and disclosure of PHI in order to perform treatment, payment or healthcare operations.  Keep in mind that while the Privacy Rule indicates that consents can be combined, section 164.506 requires that you must make HIPAA "visually separate", and that they must be separately signed. Implement your changes sooner rather than later -- certainly before the 2003 Privacy compliance deadline -- so that this critical compliance feature will be firmly entrenched in procedures, and any "bugs" can be worked out early on.

------------------------

## Minimum Necessary: Do it "Right," Reasonably

The minimum necessary standard requires that covered entities make "reasonable" efforts to limit access to PHI based upon the minimum information necessary to perform a particular role. This could include field level access based upon the role and an employee's "need to know." Or, for a small provider or an HCO with paper-based records it may be reasonable to permit access to an entire record to all employees. Compliance can be achieved in such instances without purchasing new information systems or redesigning registration areas.

However, larger HCOs with information systems that allow role-based menus cannot expect to remain on the sidelines. It is not unusual for systems with such capabilities to be "under-implemented" with fairly generic access granted to many roles for the sake of convenience. Practical solutions in this case would simply involve thinking through the true information needs of the role and limiting access through the use of restricted menus.

For example, it is not uncommon for the "Information Desk" role to be staffed by volunteers or security staff who have computerized access to a health information system's (HIS) "alpha census" in order to direct friends and families to patient locations. However, a typical alpha census not only includes patient location information but also includes information such as provider name, admission service, diagnosis, financial class and insurance information. This is clearly more information than is necessary to perform a general information desk role.

Working with a Washington, DC suburban hospital client, our staff recently solved this problem by creating an Information Desk menu. The menu replaced the alpha census with a simple "phone list" that only listed the patient's name, room number and telephone extension.

------------------------

## Right to Request Restrictions: Be Practical and Cost Effective

Patients have the right to request HCOs to communicate health information to them by "alternative means" or at "alternative locations".  A reasonable solution for small providers may be to add an additional address section on registration forms that states: "You may contact me at _______." The section would also include alternate email addresses and telephone numbers. Larger providers could reasonably build this section into customer-defined" registration system screens.

It is important to recognize that in most HCOs, recording the above information is not as big a challenge as is making sure the information is used correctly thereafter. Attention should be given to how the information will be stored, and to ensuring that the system will use it for all future correspondence and contacts.

Patients also have the right to be "de-listed" so that their names don't appear on system or printed patient listings. The Information Desk menu example cited above solved this problem by excluding patients who make such a choice. Patient Access staff flags these patients as "confidential" during the admissions process. Like many hospital information systems, the MEDITECH system used by the client hospital above can restrict the ability to view "confidential" patient information by menu and by profile. Since the Information Desk menu was designed as a restricted menu, patients who choose to be de-listed do not appear on any viewable or printable list generated from this menu. Similarly, building "minimum necessary" profiles for nursing unit staff restricts their ability to view the information of patients on other nursing units. It is important to note however, that this functionality was not designed to make systems "HIPAA compliant." The functionality is typical of today's health information systems and representative of a cost-effective means of leveraging what is for many, existing functionality.

------------------------

## The Physical Environment: Combine Better Service with HIPAA Solutions

### SIGN-IN LOGS

Though the Privacy Rule is still ambiguous on this issue, you can take steps now towards HIPAA compliance that will also enhance customer service. One solution we recently implemented was to replace sign-in logs with individual sign-in sheets that include seating maps of the waiting area. The front-desk staff will continue to greet patients and request that they print their names and appointment times. But check-off boxes have been added to the form so that patients can indicate the department they intend to visit without being asked. To avoid having to call out patient names, once patients are seated, the front-desk staff now note their location in the waiting room on the seating maps and places the sign-in sheet in a "to be done" bin for the registration staff. Access staff then uses the seating maps to locate the patients in the waiting room, and without announcing their names, approaches and escorts them back to the registration area.

In offices that offer less mobility for access staff, include a consent line on sign-in sheets that authorizes the staff to call patient's names in the waiting room.

A less personal but effective solution might involve the use of "silent" paging systems to alert patients and families. Not only can such systems help protect patient confidentiality but they also provide the following added customer service benefits:

* Noise reduction in waiting areas
* Alerts to families when a patient's surgery is finished
* Freedom for families and patients to use hospital amenities while waiting
* Elimination of mispronounced names

### INTERVIEW BOOTHS AND TREATMENT ROOMS

A variety of solutions exist for providing confidential registration interviews. If feasible, a patient registration interview area would optimally include rooms or "booths" with doors that could be closed to conduct interviews. Attractive modular units can be erected in as little as one day. HCOs that conduct bedside registration, such as our suburban DC client, are considering individual treatment rooms in the redesign of their emergency department. But a low-cost alternative might be to install sound reducing partitions between registration windows while training access staff to speak quietly during their patient interviews.

## INTERVIEW DO'S AND DON'TS

What if you work in a small office that collects most patient information at a "front desk?" Observation of a few simple "dos and don'ts" will help you to achieve compliance even when the setting is not very privacy-friendly:

* DON'T verbally collect patient information while patients are queued up in lines at the desk.
* DO use individual patient sign-in/seating map sheets such as the one cited earlier to allow patients to silently sign themselves in.
* DO ask each patient to be seated. Patients may then be either called or escorted to your desk (one at a time) to be quietly and confidentially interviewed.

## LOOSE DOCUMENTS: RE-THINK OLD METHODS

Many paper records originate in the patient access department. Original copies of facesheets, prescriptions and consent forms are collected by patient access staff and forwarded to medical record departments for permanent storage. Other departments such as Case Management and Patient Accounting may want copies of insurance cards and managed care referral forms. These documents are copied, collated and temporarily stored at a patient access front desk or on an open file on the desk of the typical access clerk. When the access clerk excuses herself to make copies, the documents obtained from previous patients are at risk of being viewed by her current patient.

One solution to consider: go paperless. Scanners have become very low-cost. Staff will not only spend less time on a close-at-hand desktop scanner than at a centrally located copier, but will not need to abandon their post to create the scanned copies. An added benefit of scanning is that with many document imaging programs, "minimum necessary" workflows can be built that automatically archive scanned documents and route them directly, only to the users that need them.1

A simple, but practical solution for small providers might be to use hanging desk drawer files for temporary storage of paper documents. The drawer can be closed when that inevitable trip to the copier must be made.

Shredders can also be used effectively to destroy documents that are no longer needed. But they can be expensive if you must destroy volumes of documents at numerous points of service. A practical solution may be to purchase one or two high quality, high volume shredders. Access areas can be provided with covered "shred only" containers that are emptied daily by housekeeping staff who are trained to properly dispose of materials using the high-volume shredders.

-----------------------

Provider Scheduling of First-Time Patients with HCOs: Build on What You Already Have

The Privacy Rule does not allow covered entities to use PHI prior to obtaining written consent for TPO. This poses problems when providers must directly schedule first time appointments or procedures with HCOs. As with consent, a practical solution would build upon systems that are already in place. For example, since many HCOs provide order forms and pre-registration forms to local referring providers, the HCO's consent form could be incorporated into these documents and be signed by the patient prior to scheduling appointments or procedures. Again, remember to make these HIPAA consents visually separate, and provide a space for a separate signature.

-----------------------

Thinking Ahead:  Training, Training, Training

Probably the most reasonable and cost-effective measure that you can take right now to ensure patient privacy would be to send a clear message to your access staff by beginning training, and consistently reinforcing it. Start with sessions to raise the staff's awareness of the privacy requirements. Awareness training can help raise their privacy antenna, and get their mental wheels turning, thereby encouraging staff to begin thinking about potential, practical solutions for their particular environment. Early staff meeting awareness sessions will also "grease the skids" for the enterprise's more formal, official training program. Your smaller, department-based sessions can be done informally and interactively at weekly staff meetings, where incremental bits of learning can be provided, perhaps for just 20 minutes at a time, covering specific, critical features of patient-access privacy issues. You might leave user-friendly written material - such as a relevant HIPAAnote - with your staff to reinforce the goals of the session.

A high-impact prelude to your first training session might be to have a person from another department walk through your department and document or collect every piece of PHI that they can get their hands on. All of the collected PHI could be brought to the first meeting to sensitize the staff to the risks faced in their own work areas. Consider ending these sessions with a bit of brainstorming; you'll generate good ideas and solutions, while at the same time reinforcing staff buy-in to the need for and value of better privacy practices.

"Getting it right" on the front end in patient access is often a critical component of good revenue cycle management.  Getting HIPAA right" will be no different, because HCOs will depend heavily on patient access staff to meet many of the challenges of compliance. Fortunately, as the examples cited above illustrate, these challenges can be met in reasonable and cost effective ways that build upon what many HCOs are already doing and enhance service delivery in the process.

-----------------------

John Thompson, Director, Phoenix Health Systems, is currently leading a longterm outsourcing engagement as Patient Access Director for an integrated health system, responsible for directing major departmental systems and process enhancements. Phoenix is expert in HIPAA change management, strategic planning, and procurement, implementation and integration of state-of-the-art health care information technology. http://www.phoenixhealth.com

============================================================
==============

4 >> HIPAA / EDI: Q/A on Transactions & Code Sets

** Employer Identifers With and Without the Hyphen **

by Kepa Zubeldia, M.D., President/CEO of Claredi

QUESTION: Do I really need to use the hyphen when identifying a provider with the EIN?

ANSWER: We have received a formal clarification from the Department of Health and Human Services (HHS) on the use of the standard Employer Identifier. In fact, the clarification contradicts my previous HIPAAlert note, so this is a correction that will hopefully clear the air and will let some of us sleep easier.

According to Pat Peyton, the HHS contact for this rule, "the employer identifier standard (i.e., the EIN with the hyphen) is used in the standard transactions when the employer needs to be identified."

The key is that the entity being identified by the employer identifier standard must be acting in the role of employer. So if the entity being identified is a provider, or a payer, or another entity, that is not in *the role* of employer, the hyphen is not required even if the ID used to identify that entity is the EIN. For example, the email from Pat clarifies that "if an employer is an "Information Source" or an "Information Receiver," that employer would not be acting in a role of an employer (but would simply be an "Information Source" or an "Information Receiver"). As such, the EIN (i.e., without the hyphen) could be used because the Employer Identifier Final Rule would not apply to this use of the EIN."

(The email correspondence with Pat is much longer than the excerpts shown. I will spare you the details of all the emails going back and forth.)

Interestingly enough, Pat also says "We have already acknowledged that an employer is not a covered entity and, therefore, need not use the employer identifier standard (i.e., the EIN with the hyphen) to identify itself or any other employer in a standard transaction and need not even use a standard transaction."

So, is there any situation when the hyphen MUST be used in the EIN?

Pat says: "As best we can tell, the only situation where a covered entity is obligated to follow the format as established in the Final Rule (i.e., the EIN with the hyphen) is in the 834 in this situation: The sender is a plan sponsor who is not an employer (because an employer is not required [...] to use the standard transaction [...]) and, in the transaction, the sponsor is identifying the employer of the member being enrolled or whose enrollment is being modified."

I don't know how frequent that case will be, but it seems to me that the conclusion is that the receivers of the 834 transaction need to be able to receive the hyphen in case some of the employers choose to use the standard. Other than that, it is still up to the industry to decide whether to send punctuation or not send it as part of the identifiers. So we have the HIPAA employer identifier standard (the EIN with a hyphen), and we also use the EIN without the hyphen (just the 9 digits) when we need to identify someone in a role other than employer. That use of the 9-digit EIN without the hyphen is a simple industry convention, not a HIPAA standard.

------------------------

Kepa Zubeldia, M.D., is President and CEO of Claredi, a leading provider of HIPAA EDI compliance testing and certification. http://www.claredi.com

========================================================================

5 >> HIPAA / LAW : Legal Q/A

** How HIPAA Security Applies to Transcriptionists **

by Steve Fox, Esq., & Rachel Wilson, Esq., Pepper Hamilton LLP

QUESTION: To what extent are medical transcriptionists required to comply with HIPAA?

ANSWER: Medical transcriptionists are required to implement reasonable safeguards designed to protect the privacy and  security of personal health information (PHI).

Medical transcriptionists are subject to the business associate requirement set forth under HIPAA's privacy rule (the "Privacy Rule"). They are subject to this requirement because the transcriptionist performs a function on behalf of health care providers that includes the use and disclosure of PHI. Accordingly, transcriptionists are prohibited from using or disclosing PHI in any manner that would violate the Privacy Rule if done by the provider itself. It is important to keep in mind, however, that covered entities, although not allowed to use or disclose PHI in any manner except as permitted under HIPAA, are not required to protect against any and all, known, unknown, or unlikely uses or disclosures in violation of the Privacy Rule. Safeguards must be reasonable, but not foolproof.

HIPAA's proposed security standards (the "Security Standards") apply to PHI that is either electronically maintained or transmitted. Covered entities will be required to enter into chain of trust agreements with medical transcriptionists when PHI is processed electronically through the transcriptionist. (Of course, this assumes that the "chain of trust" concept remains in the final rule.) Pursuant to these chain of trust agreements, transcriptionists will be obligated to maintain the integrity and confidentiality of PHI while in receipt of such information and during transmission of the same. HIPAA falls short of mandating specific technology solutions that covered entities must implement (or require of their chain of trust partners to implement), in order to ensure the security of PHI; requiring only that covered entities implement appropriate administrative procedures, physical safeguards, and technical security services and mechanisms to guard data integrity, confidentiality, availability and to prevent unauthorized access to certain data.

Read past HIPAA Legal Q/A articles:

http://www.hipaadvisory.com/action/LegalQA/archives.htm

----------------------------
Clarification: In last month' s article, we stated that employer sponsors of group health plans generally have certain compliance obligations under the Privacy Rule as business associates. This statement resulted in some confusion among HIPAAlert subscribers. The sentence should have read, "Employer sponsors of group health plans have certain compliance obligations under the Privacy Rule as do business associates." The point we intended to make is that, much like the business associate requirement under the Privacy Rule, covered entities are required to obtain certain written assurances from employer sponsors related to the use and disclosure of PHI.
----------------------------

Steve Fox, Esq., is a partner at the Washington, DC office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., of Pepper Hamilton LLP.
http://www.pepperlaw.com/
Disclaimer: This information is general in nature and should not be relied upon as legal advice.

=========================================================================

6 >> HIPAA / SECURE: Security Q/A

** The Best Way to Develop Security Policies **

by Eric Maiwald, CISSP, Fortrex Technologies

QUESTION: Based on the proposed HIPAA requirements, we know that we will need to develop security policies. What is the best way to go about this?

ANSWER: There are several issues that need to be addressed when writing policy. Even before you start writing, make sure you understand the culture of the organization. The culture of the organization will help you to define acceptable behavior (especially in terms of Internet and computer use).

As you begin to work on policy, try to identify how the policies will fit together. Writing a low level procedure may turn out to be the easiest, but it may impact how higher level corporate policy may be written. Therefore, starting with some of the higher level documents may be more appropriate.

Once you have decided where to start make sure you include stakeholders in the process. A stakeholder is someone who has a vested interest in what the document says and how it will be implemented. I have seen a number of cases where policies (and occasionally entire security departments) have failed because the process did not include influential stakeholders from other departments.

Since the policies are security issues, security should drive the process. Bring the stakeholders together and provide them with an outline for the policy in question along with some points to be covered in each section. Discuss each point with the stakeholders. If you have stakeholders who want to water-down the policy too much, explain to them the risks to the organization and why the policy needs to be appropriate to help manage the risk. After the meeting, go off and put text to each section. Send the text out for comment and go over the comments with the stakeholders at the next meeting. Continue this process until you have a general consensus from the group. Then you have something you can take to management for final approval.

Once you have approved policies you will need to implement them across the organization. Please resist the temptation to just "make it so." It is important to begin awareness training with  employees before you implement policies that will impact them. For example, if you decided to change the password policy for the organization without showing employees what the new policy will be, it is likely that your organization's help desk will be overwhelmed with calls when the new policy goes into effect.

---------------------------

Eric Maiwald, CISSP, is Chief Technology Officer of Fortrex Technologies, which provides information security management, process and monitoring services for healthcare organizations and other industries. http://www.fortrex.com

=================================================================

=================================================================

=================================================================

COMMENTS? Email us at info@phoenixhealth.com
SUBSCRIBE? Visit http://www.hipaadvisory.com/alert/
ARCHIVES: http://www.hipaadvisory.com/alert/archives.htm

=================================================================

=================================================================

===================================================

=
You are currently subscribed to hipaalert
as:  kmckinst@dmhhq.state.ca.us
======
To view the list's archives, change your settings (e.g., your email address, switch to HTML or text version, set to 'nomail' while you're away), or UNSUBSCRIBE, go to:
http://lyris.dundee.net/cgi-bin/lyris.pl?enter=hipaalert